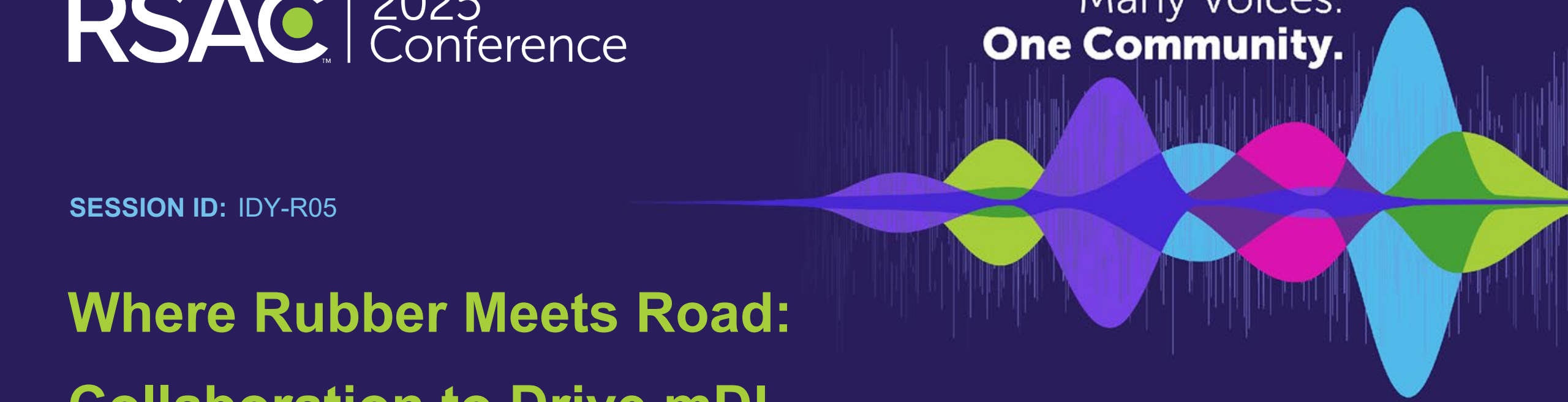
RSAC 2025 Conference

Many Voices. One Community.



SESSION ID: IDY-R05

Where Rubber Meets Road:

Collaboration to Drive mDL Standards and Adoption

Ryan Galluzzo
Identity Program Lead
National Institute of Standards and Technology

Nicholas Hazelbaker
Security Architect
JP Morgan Chase

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

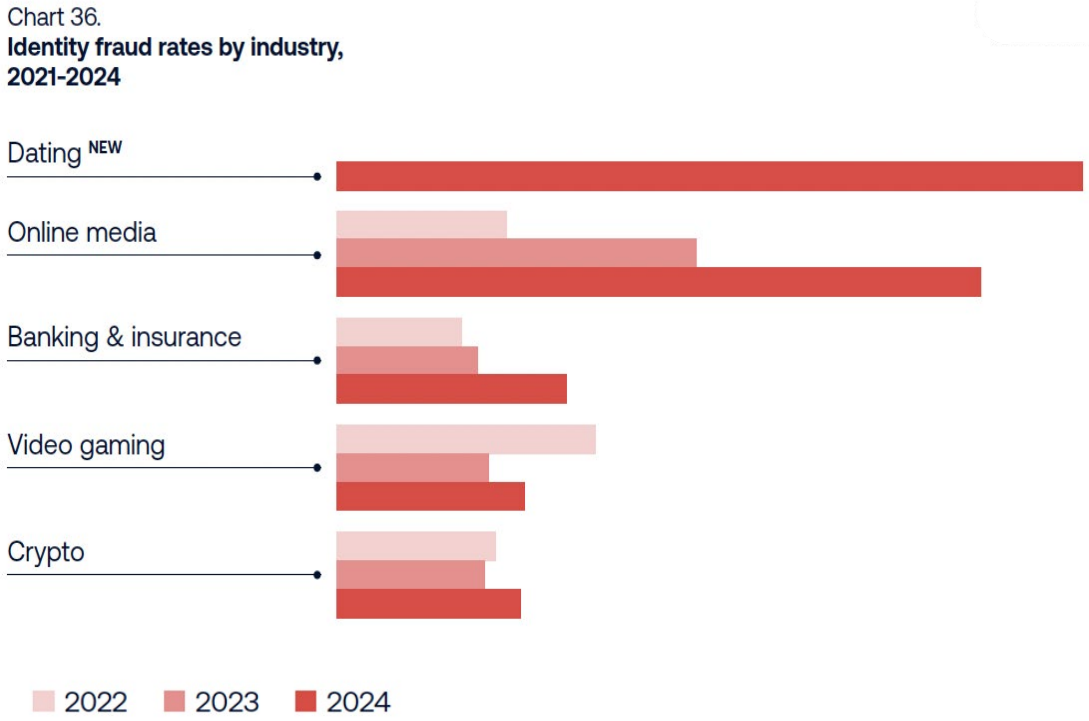
This information is provided for discussion and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed here in. These materials do not represent an offer or commitment to provide any product or service. It does not provide a comprehensive list of all types of cyber threats, and it does not identify all types of cybersecurity best practices. you, your company or organization is responsible for determining how to best protect against cyber threats and for selecting the cybersecurity best practices that are most appropriate to your needs JPMorganChase assumes no responsibility or liability whatsoever to any person in respect of such matters.

RSAC 2025 Conference

Impact of Identity Related Fraud

Impact – Identity Related Fraud

- **Knowing who you are interacting with online is hard** and when you don't know you expose your self to increased risk of fraud.



In January 2024, FINCEN published a report highlighting $351 billion dollars in fraud attributed to identity-related suspicious activity reports.

Identity Exploitation	Number of BSA Reports	Total Suspicious Amounts
Impersonation	1.7 million	$200 billion
Compromise	~446,000	$112 billion
Circumvention	~323,000	$39 billion
Total	**2.4 million**	**$351 billion**

Exploitations Reported in Identity-Related BSA Reports

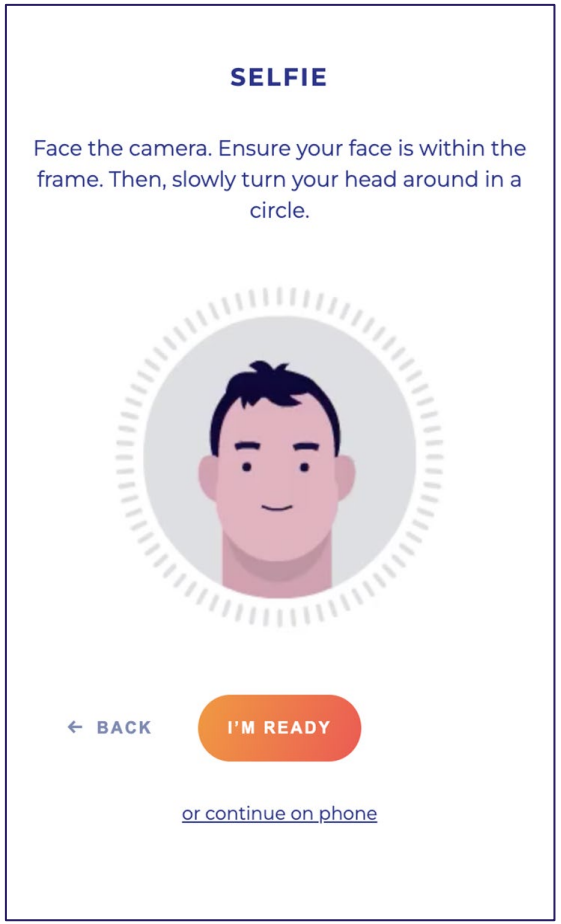
(Source: https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf;; Source: https://sumsub.com/guides-reports/identity-fraud-report-2024-2025/)

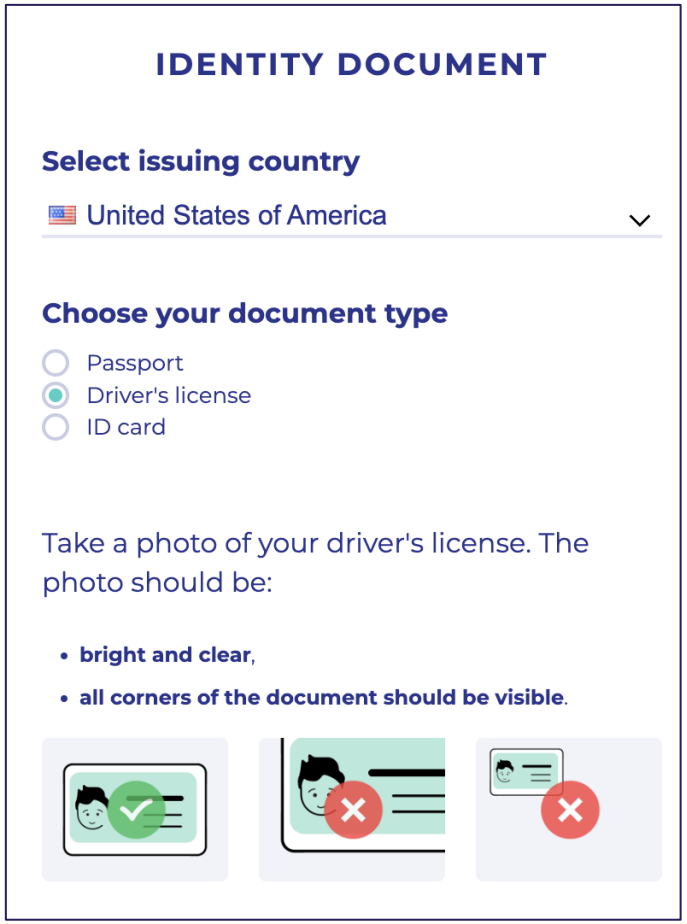
RSAC 2025 Conference

Current Challenges With Online Identity Verification

Today, Identity Verification is…

- KBA
  - Commonly verified with credit bureaus
- Upload a Photo of passport or Driver's license
  - Commonly verified with software
- Server-side Facial Match
  - Checked against portrait on Passport or DL


SELFIE
Face the camera. Ensure your face is within the frame. Then, slowly turn your head around in a circle.
BACK
I'M READY
or continue on phone


IDENTITY DOCUMENT
Select issuing country
United States of America
Choose your document type
Passport
Driver's license
ID card
Take a photo of your driver's license. The photo should be:
bright and clear,
all corners of the document should be visible.

Physical IDs can be…

- Lost/Stolen
- Counterfeit
- Issued to illegitimate user

TEXAS NEWS

Criminals stole thousands of Texans' identities and ordered fraudulent driver's licenses. Here's what to do if you're a victim

(Source: https://www.wfaa.com/article/news/local/texas/texans-identities-stolen-fraudulent-drivers-licenses-heres-what-to-do-if-youre-a-victim/287-abec4d05-a63b-4bfd-8ec0-751a8e54f99c)

Physical to Digital…

Considerations

- Fakes are increasingly high quality
- Security elements don't provide much assurance online.
- Quality and capture impact the ability to authenticate and ID.
- Data checks to confirm validity and accuracy are challenging
- Image capture to user provided evidence is unreliable
- End user privacy expectations are increasing

Challenges with Physical Licenses

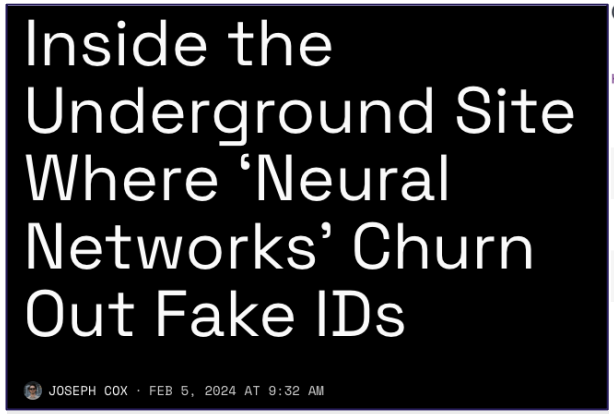
- Issuer can invalidate but not revoke the physical license once issued
- High quality counterfeits of driver's licenses can be made in as little as two weeks after a new license template is put into circulation
- Adversaries have scaled attack paths which can defeat photo-based DL verification
- DL images can be synthesized or phished for use by an unauthorized party
- Physical DL or image of the license does not contain chain of trust information from issuer
- End user privacy expectations are increasing
- UX implementation of DL image capture is difficult and unintuitive to users
- All data present on a license may be captured in image or manual verification

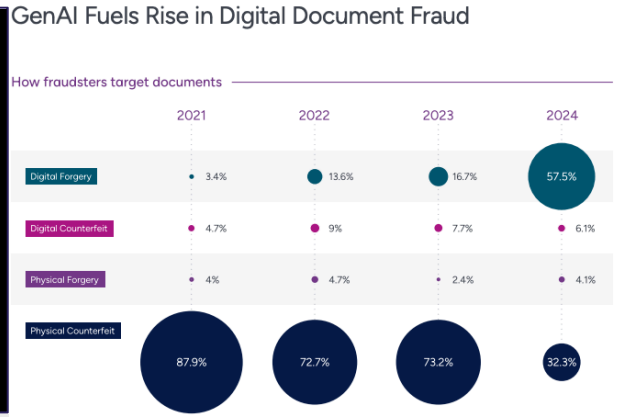
(Source: https://idscan.net/blog/which-states-include-microprint-as-a-security-feature-on-their-id/

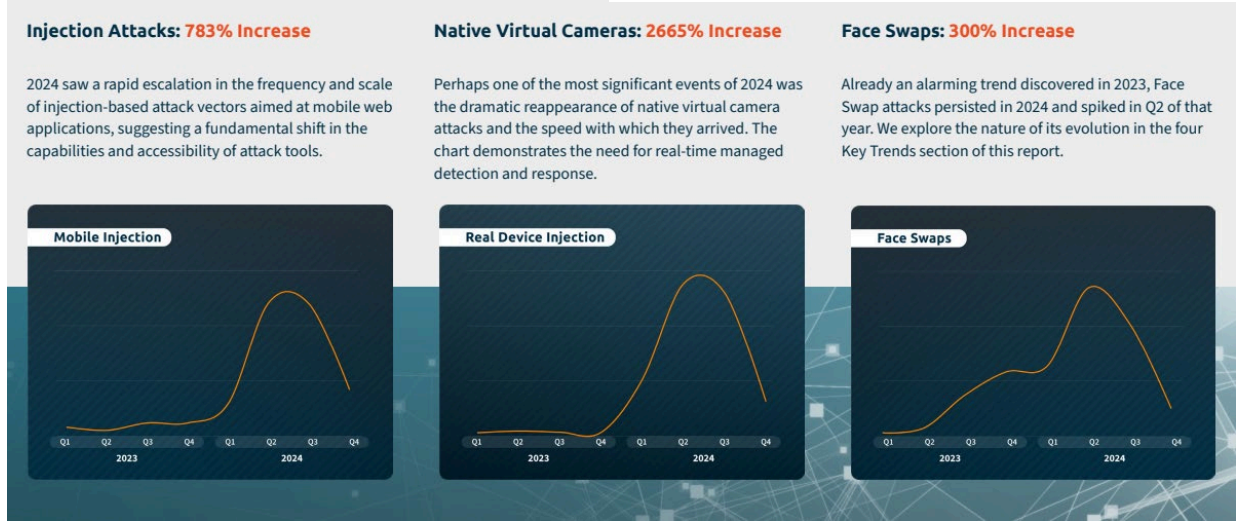
But Wait… There's More!

Queue the obligatory AI slide!

- New Threats:
  - AI generated images of fake documents
  - Deepfake video to defeat face recognition & liveness
  - Goes beyond IDV to social engineering attacks
  - ***Industrial level scale…***






Injection Attacks: 783% Increase
2024 saw a rapid escalation in the frequency and scale of injection-based attack vectors aimed at mobile web applications, suggesting a fundamental shift in the capabilities and accessibility of attack tools.
Native Virtual Cameras: 2665% Increase
Perhaps one of the most significant events of 2024 was the dramatic reappearance of native virtual camera attacks and the speed with which they arrived. The chart demonstrates the need for real-time managed detection and response.
Face Swaps: 300% Increase
Already an alarming trend discovered in 2023, Face Swap attacks persisted in 2024 and spiked in Q2 of that year. We explore the nature of its evolution in the four Key Trends section of this report.
Mobile Injection
Real Device Injection
Face Swaps
Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4
2023
2024

(Sources: https://www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/,https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial, https://go.iproov.com/rs/891-TPZ-847/images/iProov_Threat%20Intelligence%20report_1%202025%20%281%29%2027Feb%20DS%20v3-%20FINAL%20%281%29.pdf?version=0,, https://www.entrust.com/sites/default/files/documentation/reports/2025-identity-fraud-report.pdf)

RSAC 2025 Conference

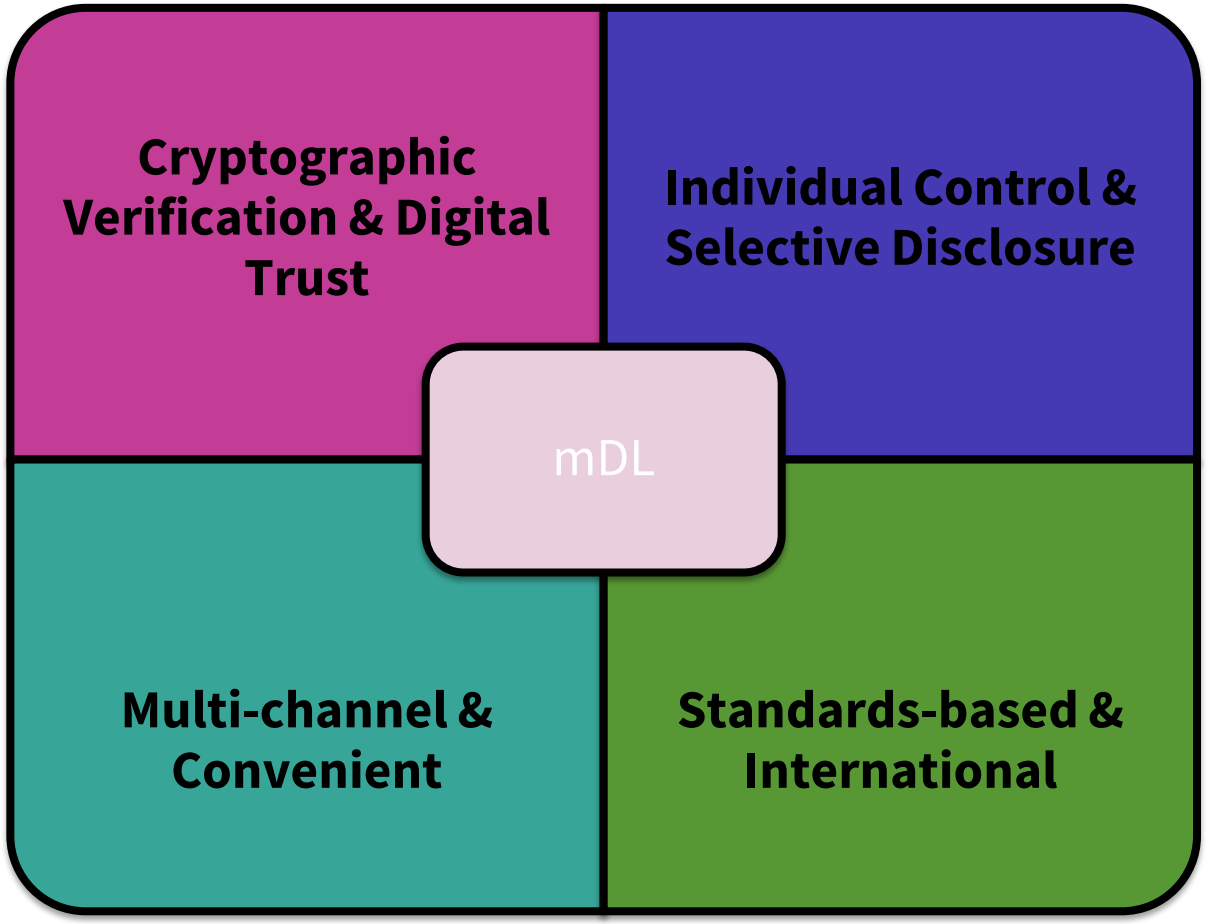
What Are mDLs and Why You Should Care

What is an mDL?

What is an mDL?

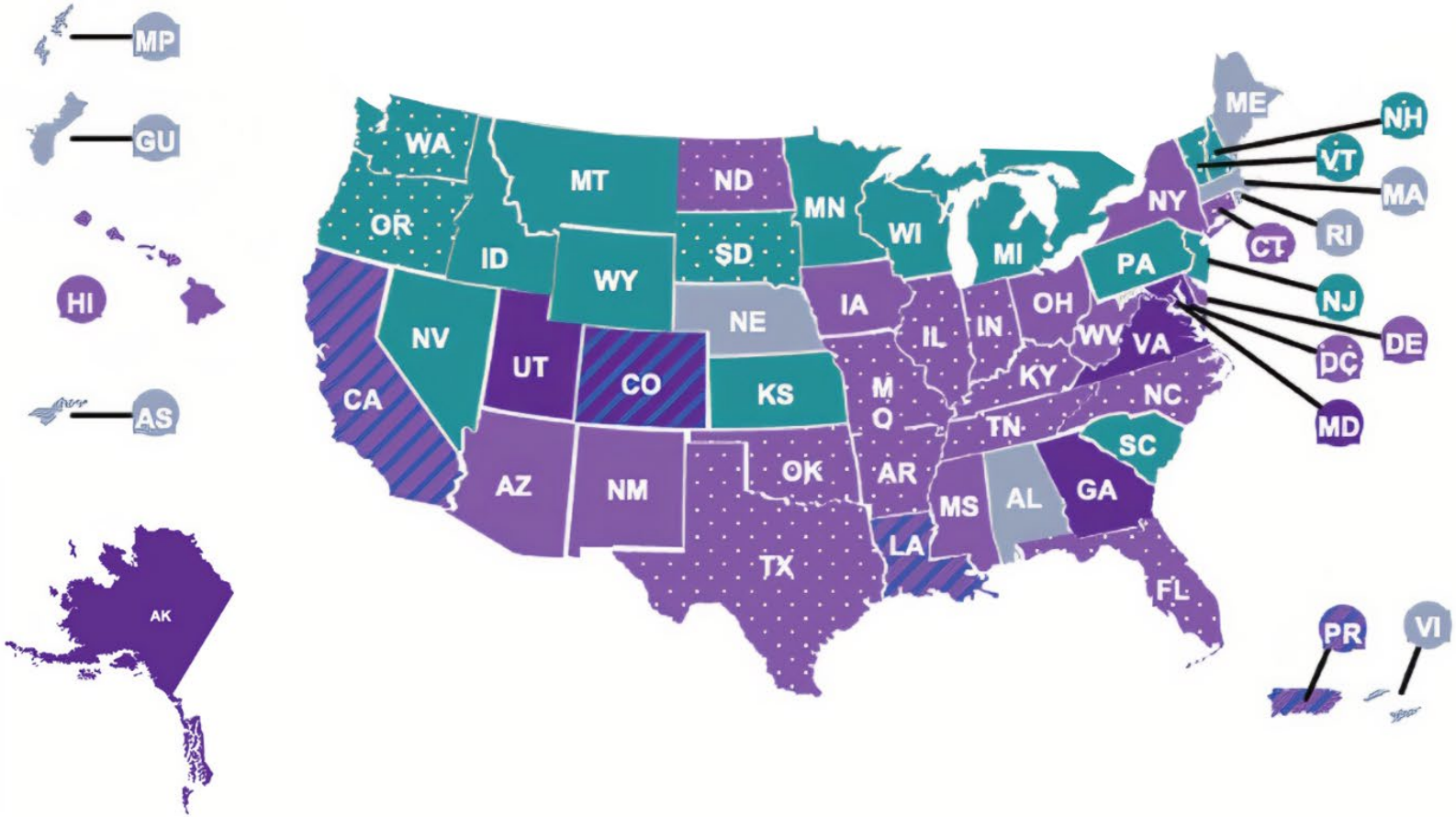
- Digital representation of your physical ID
- Issued by DMV
- Stored in a Digital Wallet
- Presented online or in person
- Cryptographically verifiable

Security Properties & Benefits



- Make use of Digital Signatures to support integrity of the data from the issuing source
- Answer questions such as “are you older than…?” without revealing age, DoB, etc.
- Leverage modern authentication to provide confidence in identity of the user presenting it
- Eliminates need to directly communicate between the RP and Issuer at each transaction
- UX gains including auto-fill, less friction, and cross device communication

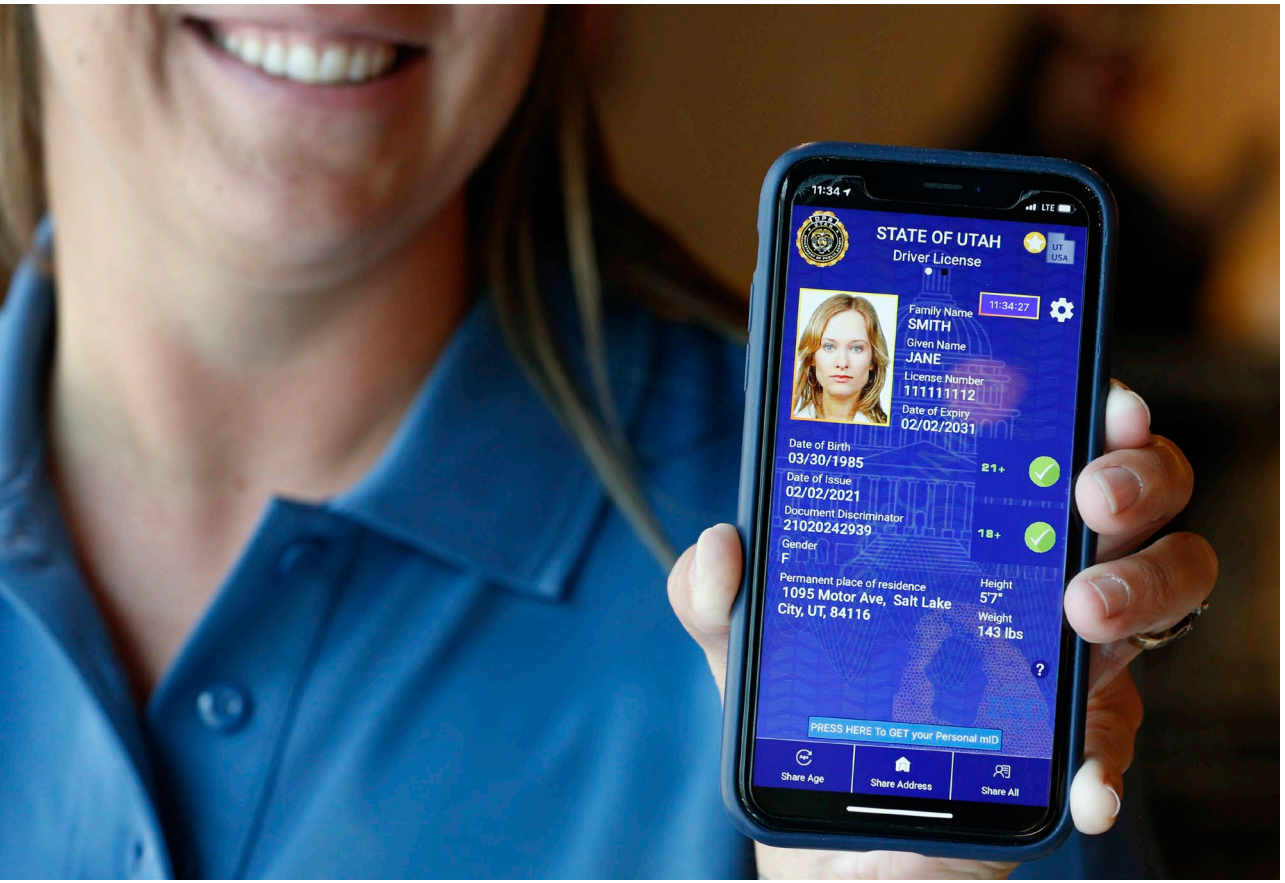
Current mDL Ecosystem



- Interoperable implementation
- Interoperable implementation in progress
- Jurisdiction specific implementation
- Public Key Available in Digital Trust Service
- Legislative and/or study activity
- Attempt to execute legislative and/or study activity
- No information available

Source: American Association of Motor Vehicle Administrators (AAMVA)

Where Can I Use My mDL?



- mDLs are accepted at select TSA Pre Check Security check points around the nation
- If your state offers mDLs, you can enroll now and try it at SFO on your flight home
- Some airports, such as BWI, allow mDLs for age verification at bars and restaurants well

RSAC 2025 Conference

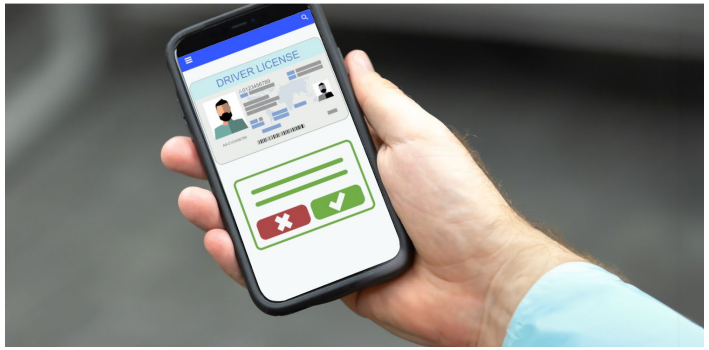
Why Financial Institutions Care About mDLs

Why Financial Institutions Care – Customer Support In-Person

- Allow service reps to focus on customer. Security and convenience in moments that matter
- Not vulnerable to high quality fake ID
- Privacy improvements for customer

Without MDL

With MDL

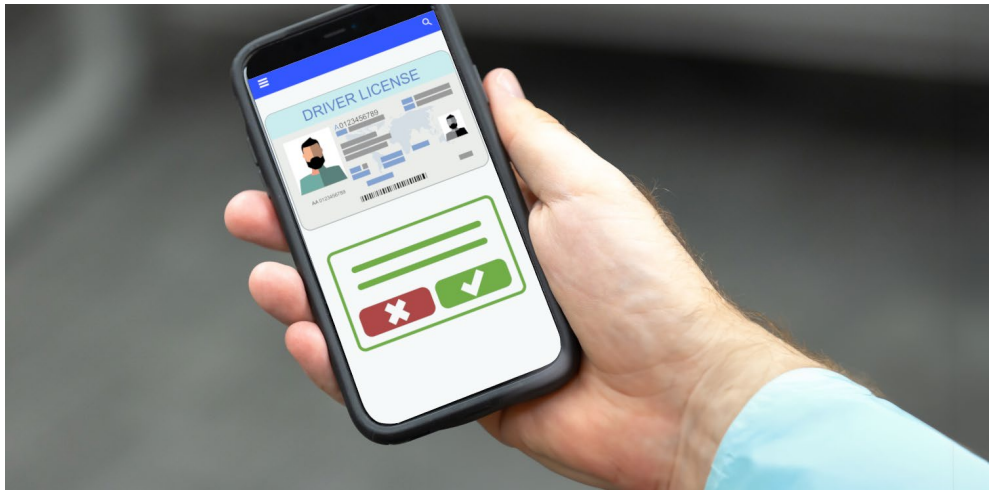


Why Financial Institutions Care – Customer Support Online

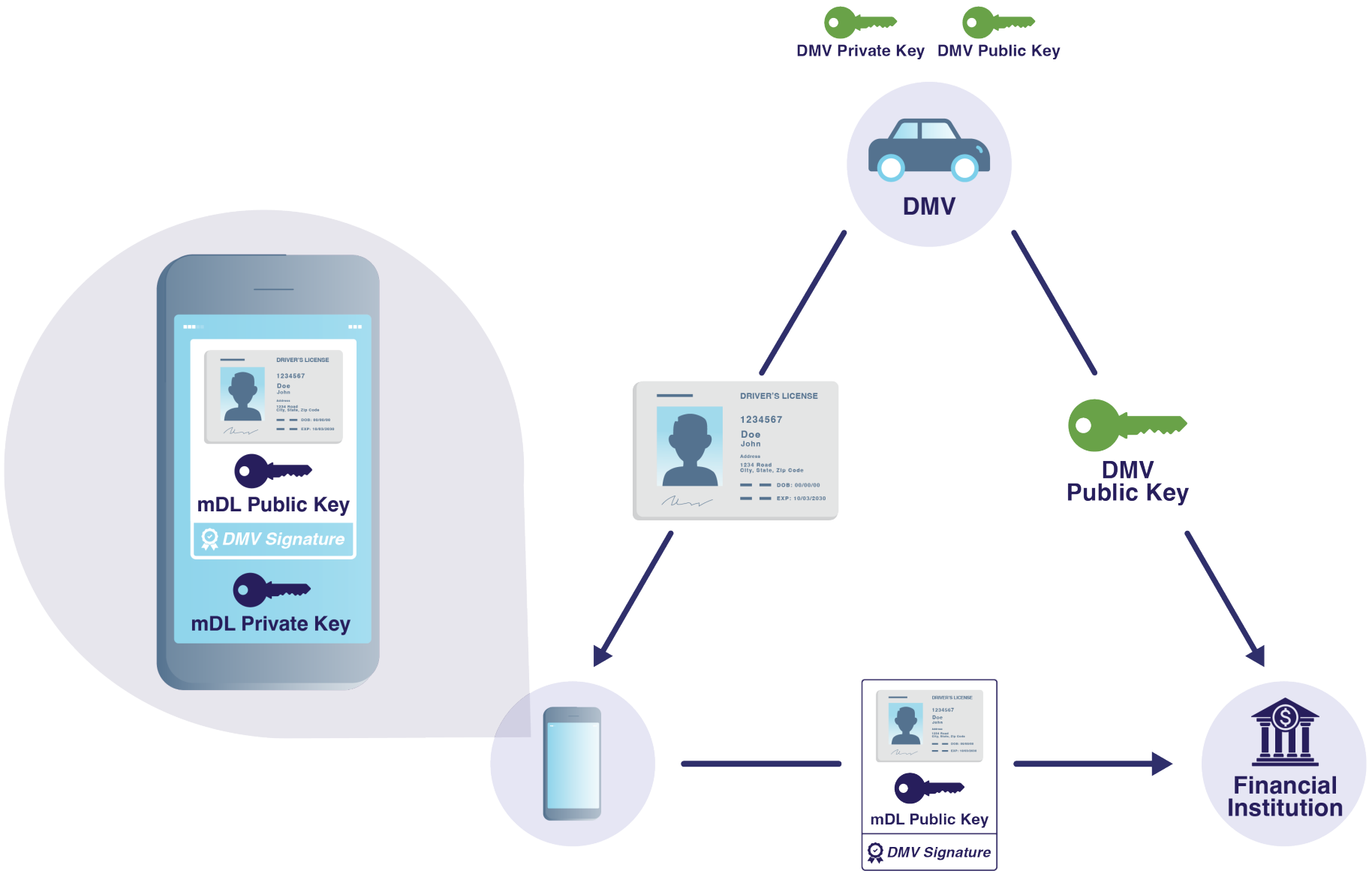
- Simpler for a customer to perform. *Not impacted by lighting, camera, or background*
- Not vulnerable to synthetic injection
- Privacy and security benefit

Without MDL

With MDL

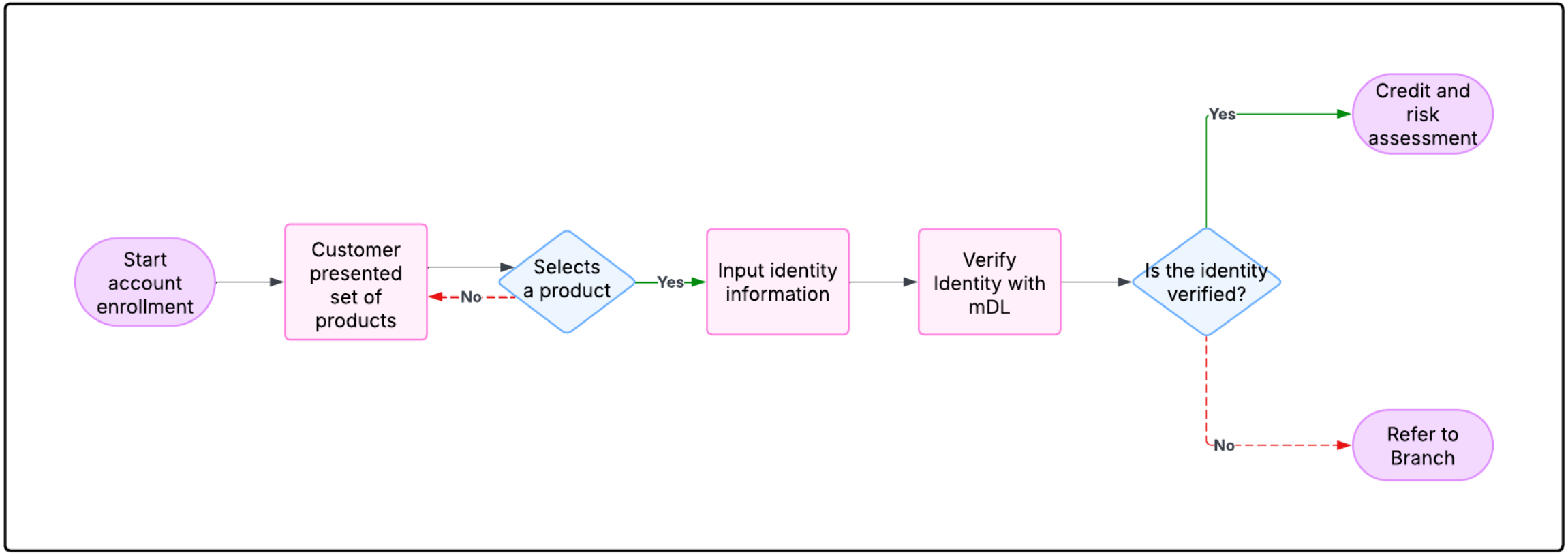


Why Financial Institutions Care – Security Benefits



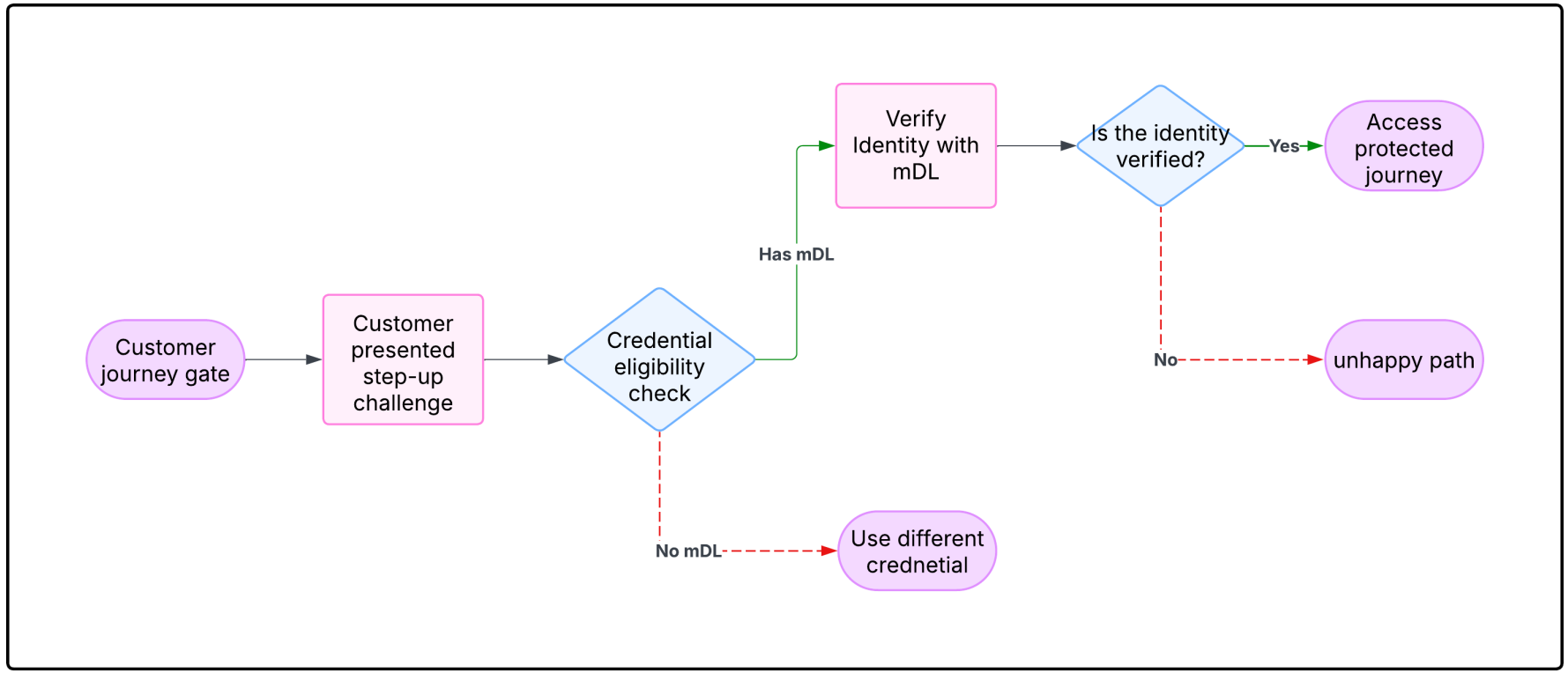
mDL Workflows of Interest to FIs: ID Verification

- Front load mDL to deflect volume from more resource / cost intensive flows



mDL Workflows of Interest to FIs: Step-Up

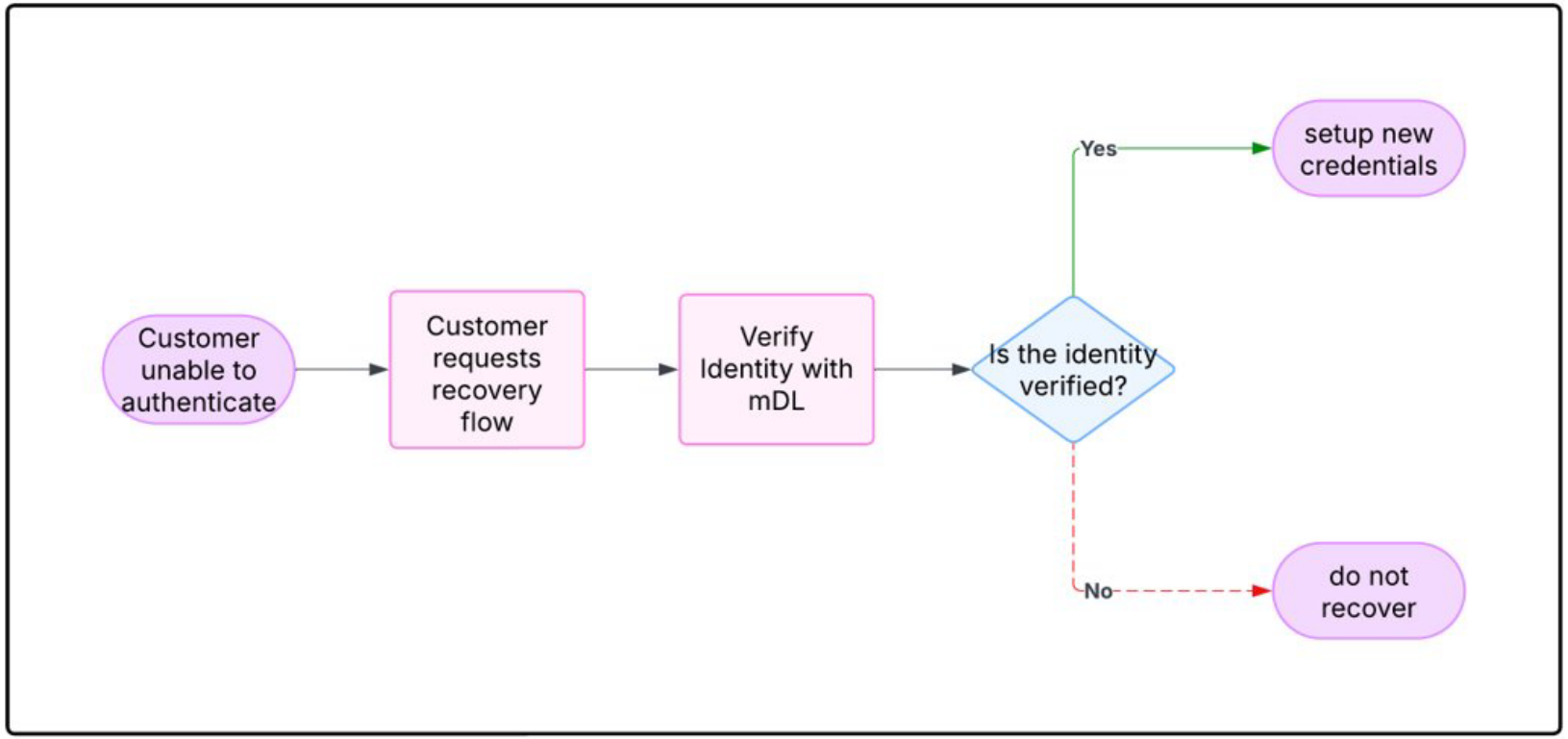
- Customer wants to access resources beyond current authorization level
- Gradual and appropriate friction
- mDL is easily sequenced with other credentials



RSAC 2025 Conference

mDL Workflows of Interest to FIs: Acct Recovery

- Consider reusing origination journey
- Can be built in combination with a step-up flow
- Useful for new credential enrollment with existing customers



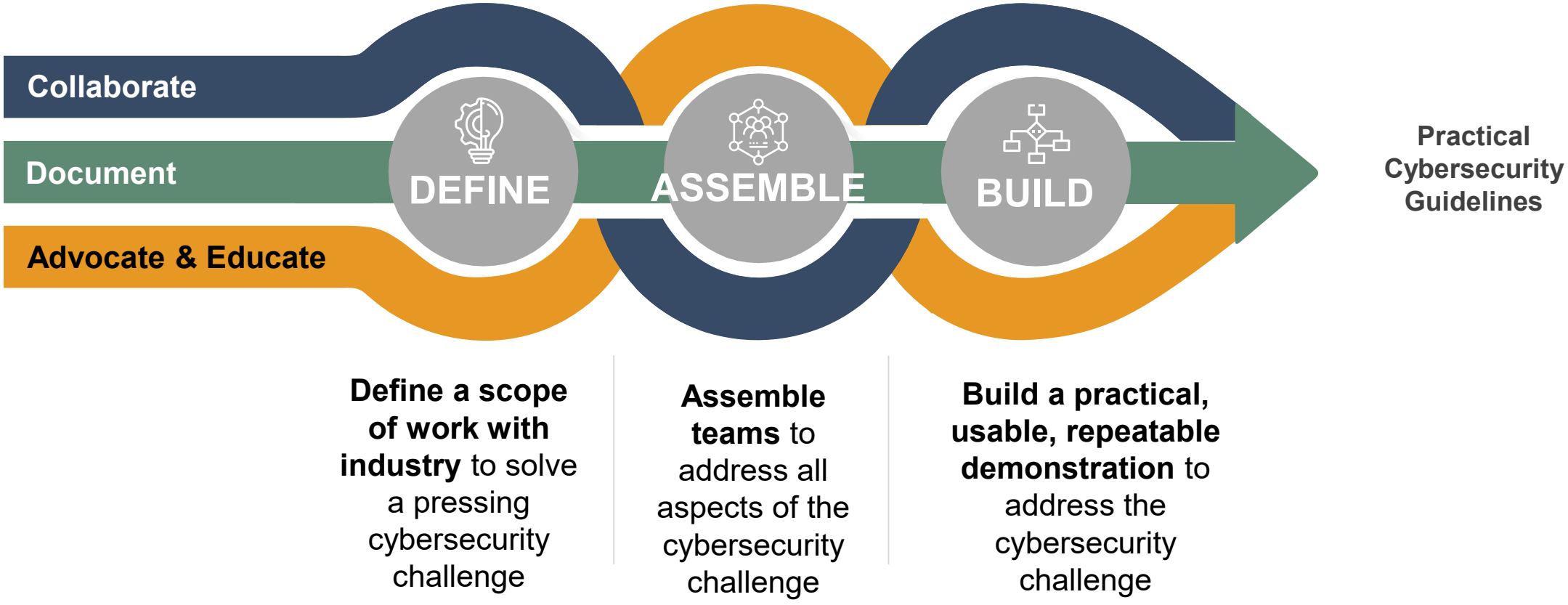
Summary of Positive Impacts to Identity Fraud

Physical DL challenge	mDL Benefit
Issuer can invalidate but not revoke the physical credential once issued	Can be revoked if fraudulently provisioned or abused
High quality counterfeits of driver's licenses can be made in as little as two weeks after a new license template is put into circulation	Cannot be physically counterfeited
Adversaries have scaled attack paths which can defeat photo-based DL verification	Removes scale from common Identity attack paths
DL images can be synthesized or phished for use by an unauthorized party	Phishing resistant
Physical DL or image of the license does not contain chain of trust information from issuer	Provides "chain of trust" information not available with a physical license
UX implementation of DL image capture is difficult and unintuitive to users	Better UX makes deployment and sequencing changes simpler
All data present on a license may be captured in image or manual verification	Reduces data security and privacy concerns impacting both the identity owner and relying party

RSAC 2025 Conference

Bridging the Gap: Collaboration to Drive mDL Adoption

What is the NCCoE?



Define a scope of work with industry to solve a pressing cybersecurity challenge

Assemble teams to address all aspects of the cybersecurity challenge

Build a practical, usable, repeatable demonstration to address the cybersecurity challenge

Transitioning guidelines into practice

Solving Business Challenges…Together

21 Collaborators

7 Banks

2 Largest US wallet providers

5 of top 10 Largest US Banks

Issuers | **Wallets** | **Verifier** | **IAM** | **FIs** | **Standards & Trust**

How the NCCoE Provides Value to FIs

- Quick onramp to understanding emerging technologies
- Full perspective from the expertise of cross industry stakeholders
- Paved path to compliance

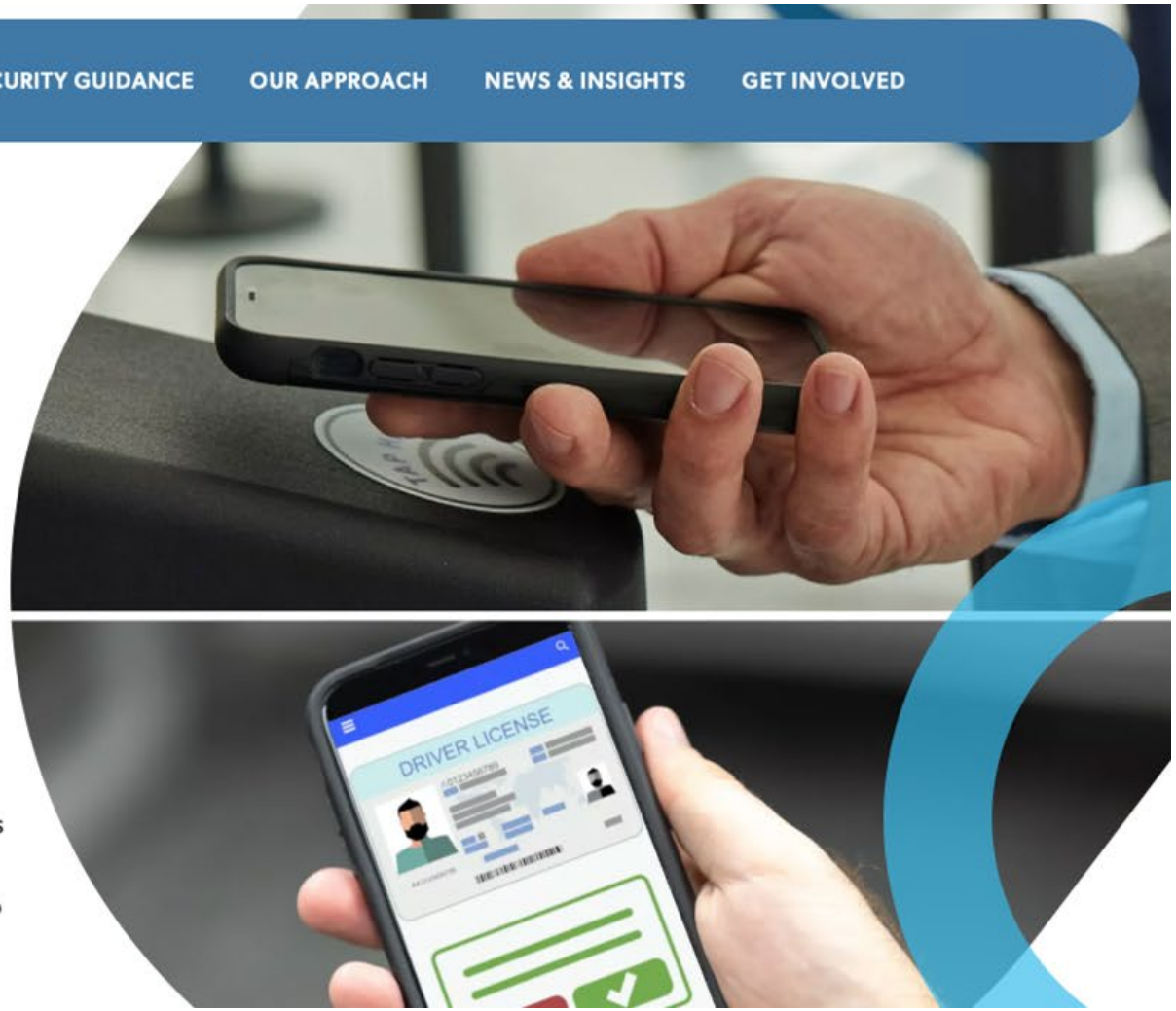
NCCoE Resources to Help FIs and You

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SECURITY GUIDANCE | OUR APPROACH | NEWS & INSIGHTS | GET INVOLVED

Digital Identities - Mobile Driver's License (mDL)

The National Cybersecurity Center of Excellence (NCCoE) is helping to accelerate the adoption of mobile driver's license standards and best practices. In collaboration with technology vendors, government agencies, regulators, standards bodies, and organizations seeking to adopt mDLs, the NCCoE will build a reference architecture demonstrating real world business use cases, integrating mDLs with commercially available technology and into business processes.



NCCoE Resources to Help FIs and You

NIST
NCCoE Mobile Driver's License Project
Search
Digital Identities - Mobile Driver's License (mDL)
Draft CIP/KYC Use Case Requirements
Submit Comments
Draft CIP/KYC Use Case Requirements
Through discussion with our project collaborators, the project team has developed a set of functional and non-functional technical requirements as the basis for our demonstration. These requirements have been gathered from sources including best practices, banking regulatory requirements, and other guidance. We are publishing these requirements for early feedback from our community of interest.
The demonstration requirements in the table below can be filtered in a few ways:
1. Grouped by the notional architecture component the requirement applies to,
2. Grouped by the requirements source where the requirement was derived from, or
3. Grouped by usability requirements, which is a focus area for the demonstration that spans web and mobile interfaces.
3. Grouped by usability requirements, which is a focus area for the demonstration that spans web and mobile interfaces.

CYBERSECURITY INSIGHTS a NIST blog
Digital Identities: Getting to Know the Verifiable Digital Credential Ecosystem
November 13, 2024
By: Bill Fisher and Ryan Galluzzo

RSAC 2025 Conference

Example User Journey

Applying for a Financial Account using an mDL

mDL Wireframe #1

Flow: Applying for a financial account.

This wireframe describes a representative user journey for a prospective customer applying to open a new financial account and using an mDL for identity proofing. What is described here is not the only way to design the flow for a user's journey. However, this is an example that can be used by financial institutions to adapt as necessary to meet the needs of their own customers and internal IT infrastructure.

Comments on the user journey can be offered at Submit Comments.

To review the other wireframes in this project and for more information please visit: Wireframes.

Start Wireframe >

Lessons Learned & Current Focus

- Trust model
- Presentation protocols
- Consent
- Education
- Differing expectations for FR
  - Some customers willing to make privacy tradeoff, some not
  - FIs will have differing tolerance

“Apply” Slide

- Now:
  - Check to see if your state offers mDLs and begin to inquire about where you can present them
  - Visit the NCCoE project page for more information:
    - https://www.nccoe.nist.gov/projects/digital-identities-mdl
- In Three Months:
  - If your organization has remote identity verification or proofing requirements, consider if mDLs could improve customer experience, enhance security and enable privacy principles.
- In 6 months:
  - Look for new NCCoE guidance on using mDL for online identity verification

Summary

- Current online identity verification techniques are insufficient
- Online identity verification is getting harder thanks to AI and Deepfakes
- mDLs are cryptographically backed credentials that could offer improve customer experience and security during online identity verification
- The mDL ecosystem is still evolving and so the NCCoE providing guidance on how mDLs can support business functions

RSAC | 2025 Conference

Many Voices.
One Community.

Thank You

https://www.nccoe.nist.gov/projects/digital-identities-mdl